Quantum Computer Condition: Stability, Classical Computation and Norms

Gerald Gilbert, Michael Hamrick, F. Javier Thayer and Yaakov S. Weinstein
Quantum Information Science Group
MITRE
260 Industrial Way West, Eatontown, NJ 07724 USA
E-mail: {ggilbert, mhamrick, jt, weinstein}@mitre.org

The Quantum Computer Condition (QCC) provides a rigorous and completely general framework for carrying out analyses of questions pertaining to fault-tolerance in quantum computers. In this paper we apply the QCC to the problem of fluctuations and systematic errors in the values of characteristic parameters in realistic systems. We show that fault-tolerant quantum computation is possible despite variations in these parameters. We also use the QCC to explicitly show that reliable classical computation can be carried out using as input the results of fault-tolerant, but imperfect, quantum computation. Finally, we consider the advantages and disadvantages of the superoperator and diamond norms in connection with application of the QCC to various quantum information-theoretic problems.

PACS numbers: 03.67.-a, 03.67.Lx, 03.67.Pp

INTRODUCTION

The Quantum Computer Condition (QCC) [1] is a rigorous mathematical statement that connects the irreversible dynamics of the quantum computing machine, with the reversible operations that comprise the quantum computation intended to be carried out by the quantum computing machine. A discussion of several physical consequences of the QCC is found in [1], including the Quantum Computing No-Go Theorem, which establishes a bound for decoherence and dissipation beyond which quantum computation is not possible.

The quantum computer condition is denoted by the symbol $\mathbf{QCC}(P, U, \mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}}\mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}}, \alpha)$. This holds if and only if, for all density matrices $\rho \in \mathbf{T}(H_{\mathrm{logical}})$, we have

$$\|\mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}}(P\cdot(\mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}}(\rho))) - U\rho U^\dagger\|_1 \leq \alpha\ . \quad (1)$$

The above expression relates a unitary operator U on a Hilbert space H_{logical} of logical qubits with a completely positive map P on a computational Hilbert space H_{comp} via the pair of superoperators $\mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}} : \mathbf{T}(H_{\mathrm{logical}}) \to \mathbf{T}(H_{\mathrm{comp}})$, $\mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}} : \mathbf{T}(H_{\mathrm{comp}}) \to \mathbf{T}(H_{\mathrm{logical}})$ which are completely positive, trace-preserving linking maps [2]. Here, $\mathbf{T}(H)$ is the Banach space of trace class operators on a Hilbert space H with the Schatten 1 norm $\|\cdot\|_1$. The relationship between P and U is crucially expressed by the parameter α which quantifies how well P approximates U. The parameter α will be nonzero for any realistic implementation of a quantum computer due to the inevitable presence of noise and the infeasibility of correcting all possible errors [3, 4].

The QCC addresses a much broader set of problems than error correction alone, by allowing for error processes to act on the state of the system during encoding, recovery and decoding operations as well as during the computation itself. Error correction theory alone does not allow for this. Importantly, the quantity α, as such, is not even defined in the theory of error correction. The presence of the crucial parameter α highlights the difference between the limited scope of error correction and the more general notion of fault tolerant quantum computing: it reflects the inevitable survival of residual errors in *any* realistic implementation of a quantum computer. It is fault-tolerance, and not merely error correction, that is described by the QCC [5]. The advantage of the QCC is that it comprises a rigorously systematic formulation that provides a *completely general framework* for carrying out analyses of questions pertaining to fault-tolerance in quantum computers, that broadens the scope of previous approaches to the subject [6].

We will find it convenient in this paper to make use of the superoperator (SO) norm defined for arbitrary linear superoperators $Q : \mathbf{T}(H) \to \mathbf{T}(H)$ as

$$\|Q\|_{\mathrm{SO}}^{\mathrm{sa}} \equiv \sup\{\|Q(\rho)\|_1 : \|\rho\|_1 \leq 1 \text{ and } \rho = \rho^\dagger\}\ , \quad (2)$$

where the superscript "sa" indicates the restriction of the domain of the superoperator Q to self-adjoint operators ρ. We may re-express the QCC given in eq.(1) in terms of the SO norm with the equivalent inequality

$$\|P^{\mathcal{M}} - G\|_{\mathrm{SO}}^{\mathrm{sa}} \leq \alpha, \quad (3)$$

where $P^{\mathcal{M}} \equiv \mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}}P\mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}}$ and G is the map $G(\rho) \equiv U\rho U^\dagger$. This is the form of the QCC that we will use in the rest of this paper.

The paper is organized as follows. We consider three applications of the QCC to problems arising in quantum computing: (1) we study the stability of quantum computation under variation of characteristic parameters, (2) we analyze the use of realistic, fault-tolerant quantum computation in enabling subsequent classical computation, and (3) we analyze the advantages and disadvantages of the SO and diamond norms as measures of the

difference between a desired operation and its physical implementation.

STABILITY UNDER VARIATION OF CHARACTERISTIC PARAMETERS

Realistic implementations of quantum computers will exhibit fluctuations and systematic errors in the values of characteristic parameters. In this Section we consider the stability of the QCC under small such variations of parameters. Although the general form of the QCC is valid for either Markovian or non-Markovian underlying dynamics, in this Section of this paper only, we restrict consideration to the case of Markovian dynamics. The system state, $\rho(t) \in \mathbf{T}(H)$, is then governed by an equation of the form

$$\frac{d}{dt}\rho(t) = A\rho(t), \tag{4}$$

where A is a (possibly unbounded) operator on $\mathbf{T}(H)$. In this analysis, we consider time-independent operators A, with A otherwise unrestricted. Then, in the sense of analytic semigroup theory,

$$\rho(t) = \exp tA\rho(0)\ . \tag{5}$$

The propagator, $P = P(t) \equiv \exp tA$, associated to A, is a completely positive, trace-preserving map.

We now consider the stability of the QCC under small, time-independent perturbations of A. As an immediate consequence of (3), the QCC has the following property:

Lemma 1 *If* $\mathbf{QCC}(P, U, \mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}}, \mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}}, \alpha)$ *holds and* P' *is a completely positive trace-preserving map, then* $\mathbf{QCC}(P', U, \mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}}, \mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}}, \alpha')$ *also holds, where* $\alpha' \equiv \alpha + \|P - P'\|_{\mathrm{SO}}^{\mathrm{sa}}$.

As a consequence of Lemma 1 we see that replacement of P with P' will result in a quantum computer implementation inaccuracy α' that is close to the original value of α if the difference between P and P' under the (self-adjoint) SO norm is small [7].

Having established Lemma 1 we may proceed with the analysis of the stability of the QCC under small perturbations of A. Suppose A depends continuously on a parameter z, with z taking values in some topological space. We denote the z-dependence of A as A_z. The continuity property of such (possibly unbounded) operators, A_z, is defined in terms of a corresponding continuity property of the resolvent

$$\mathrm{R}(\lambda, A_z) \equiv (\lambda I - A_z)^{-1}. \tag{6}$$

We now apply this continuity property of A_z to the stability of the QCC under variation of parameters. From Lemma 1, and the observation that convergence of the resolvent $R(\lambda, A_z) \to R(\lambda, A_{z'})\ \forall \lambda > 0$ implies $\exp tA_z \to \exp tA_{z'}\ \forall t > 0$, we obtain the following result:

Proposition 1 *Suppose that* $\mathrm{R}(\lambda, A_z)$ *is norm operator continuous in* z *for all* $\lambda > 0$. *Then, if for some* t, $\mathbf{QCC}(\exp tA_z, U, \mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}}, \mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}}, \alpha)$ *holds, then for any* $\alpha' > \alpha$, $\mathbf{QCC}(\exp tA_w, U, \mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}}, \mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}}, \alpha')$ *holds for* w *sufficiently near* z.

The guarantee of stability under variations in the characteristics of the dynamics is vital when studying actual experimental implementations. In practice it is effectively impossible to guarantee the perfect stability of an experimental system. However, because of the QCC stability condition exhibited in Proposition 1, we are nevertheless guaranteed successful quantum computation, albeit with a possibly larger implementation inaccuracy (*i.e.*, the replacement $\alpha \to \alpha'$). An example of instability in an experiment is the drift of the magnetic field in nuclear magnetic resonance. This causes inhomogeneity in the quantizing field, which in turn affects the decoherence of the system. Another example of instability in controlling experimental parameters arises due to the necessity of turning on and off couplings between quantum dots. The coupling depends exponentially on distance between the electrons in the dots and is nearly impossible to control precisely or repeat exactly [8]. The stability property of Proposition 1 is essential to show that quantum computation is still possible in spite of these effects.

THE QCC, QUANTUM COMPUTATION AND CLASSICAL COMPUTATION

The generic problem to which a quantum computer will be applied will not consist solely of quantum computation *per se*, but rather will be comprised of an initial quantum computation followed by a classical computation. Typically the output of the quantum computation will be utilized as input to the classical computation. Since quantum computation results in a probabilistically distributed set of outcomes, the question arises as to whether or not *reliable* classical computation can follow. An affirmative answer to this foundational question is necessary in order that algorithms such as Shor's algorithm can be applied to practical problems. A preliminary version of this foundational question is addressed in the quantum computational model formalized by Kitaev ([9], §4.1). In Kitaev's model, the initial, purely quantum mechanical computation that precedes the subsequent classical computation, is assumed to be perfectly executed with no residual errors [10]. In this Section of our paper, we extend and complete the analysis of this foundational question by considering the realistic case in which the physical implementation of the quantum computation includes residual errors. Residual errors are always present, irrespective of the existence of decoherence-free subspaces or noiseless sub-systems, since a non-vanishing residual error probability persists even after error correction is applied [3, 4].

Our extension of Kitaev's model demonstrates that reliable classical computation can follow from fault-tolerant quantum computation.

We begin by reviewing the Kitaev model [9]. This model relates: (1) each instance of a probabilistic *classical* computational problem with (2) a *quantum* computational circuit which is polynomial time computable as a function of the instance size. This relationship can be represented by a diagram:

$$\begin{array}{ccc} H_{\rm logical} & \xrightarrow{\quad U \quad} & H_{\rm logical} \\ {\scriptstyle \rm I_p}\uparrow & \boxed{p} & \downarrow{\scriptstyle \rm O_p} \\ X & \xrightarrow[\quad F \quad]{} & Y \end{array} \ . \tag{7}$$

This diagram expresses the fact that the output of the quantum computation U is intended to be used in computing the classical function F, where $F : X \to Y$ is an instance of the classical computational problem. Here $\rm I_p$ is an initialization map, which maps the classical input space X into pure states, and $\rm O_p$ is the corresponding readout map, which maps the output of the operation U onto the classical output space Y. In general $\rm O_p$ is a quantum measurement given by a projection-valued measure (or more generally a POVM) $\{\rm E_y\}_{y\in Y}$. The symbol in the center of the diagram refers to the probabilistic inaccuracy, p, associated to the output of the classical computation. The quantity $1-p$ is a measure of the probability of success of the final classical computation, for which the quantum computation provides input data [11]. The initialization map and readout maps have to be sufficiently simple (polynomial time in the input size) so that they do not implicitly hide complexity. Kitaev's formulation [9] requires that the diagram (7) be *nearly commutative* in a probabilistic sense which we now make precise.

To this end, first replace the diagram in eq.(7) (which directly makes use of pure states) with the following diagram that instead makes use of density matrices to represent the pure states:

$$\begin{array}{ccc} \mathbf{T}(H_{\rm logical}) & \xrightarrow{\quad G \quad} & \mathbf{T}(H_{\rm logical}) \\ {\scriptstyle \rm I_m}\uparrow & \boxed{p} & \downarrow{\scriptstyle \rm O_m} \\ X & \xrightarrow[\quad F \quad]{} & Y \end{array} \ , \tag{8}$$

where the action of the map G is given by $G : \rho \mapsto U\rho U^\dagger$, the action of the map $\rm I_m$ is given by $\rm I_m : x \mapsto |\,I_p(x)\rangle\langle I_p(x)|$, and $\rm O_m$ is the quantum measurement corresponding to $\rm O_p$, except that $\rm O_m$ acts on density matrices, whereas $\rm O_p$ acts directly on vectors contained in $H_{\rm logical}$. Given an input $x \in X$, the output of the quantum mechanical computation is distributed according the probability measure on Y as follows: the probability $\Pr_x(y)$ of a singleton $y \in Y$ is $\mathrm{tr}(\sqrt{\rm E_y}U\,\mathbf{I_m}(x)U^\dagger\sqrt{\rm E_y})$. Then, the *near commutativity* of the diagram in (7) (as well as of the diagram in (8)) means that for each $x \in X$, the probability measure $\Pr_x(y)$ is sufficiently concentrated at $F(x)$ so that a majority vote algorithm determines the correct value $F(x)$. In the case the output space Y is binary, it suffices there is a $p < 1/2$, such that

$$\mathrm{tr}\left(\sqrt{\rm E_{F(x)}}U\,\mathbf{I_m}(x)U^\dagger\sqrt{\rm E_{F(x)}}\right) > 1-p \tag{9}$$

for all $x \in X$. Majority voting will yield a correct result for the classical computation provided that p is sufficiently small (*e.g.*, $p < 1/2$ in the case of Y binary). This concludes our review of the Kitaev model.

We now extend Kitaev's model by allowing for the inevitable survival of residual errors in any realistic implementation of a quantum computing machine. In other words, we will extend the analysis to include fault-tolerant operation.

We consider a classical computation for fixed input size, and an implementation of a quantum computer (appropriately specified using the QCC) that is intended to provide input data for the classical computation. Inspection of the following diagrammatic restatement of the QCC,

$$\begin{array}{ccc} \mathbf{T}(H_{\rm comp}) & \xrightarrow{\quad P \quad} & \mathbf{T}(H_{\rm comp}) \\ {\scriptstyle \mathcal{M}_{\{\rm l\to c\}}}\uparrow & \boxed{\alpha} & \downarrow{\scriptstyle \mathcal{M}_{\{\rm c\to l\}}} \\ \mathbf{T}(H_{\rm logical}) & \xrightarrow[\quad G \quad]{} & \mathbf{T}(H_{\rm logical}) \end{array} \ , \tag{10}$$

shows that the completely positive map P acting on arbitrary density matrices, can implement the idealized, perfect quantum computation, $G = U\rho U^\dagger$, with an inaccuracy no greater than α, and hence enables fault-tolerant quantum computation. Recall also that Diagram (8) connects the quantum computation, G, to an intended subsequent classical computation, F. Given this, we show by combining Diagrams (8) and (10), that *realistic quantum computation* characterized by residual errors will provide a *correct classical computation*, as long as the sum $p+\alpha$ of the probabilistic and implementation inaccuracies is sufficiently small. This is formalized in the following theorem:

Theorem 1 *Suppose Diagrams (8) and (10) hold. Using the compositionality property of these diagrams, proved below, we adjoin Diagram (10) to Diagram (8) to obtain the following diagram:*

$$\begin{array}{ccc} \mathbf{T}(H_{\rm comp}) & \xrightarrow{\quad P \quad} & \mathbf{T}(H_{\rm comp}) \\ {\scriptstyle \tilde{\rm I}_{\rm m}}\uparrow & \boxed{\alpha+p} & \downarrow{\scriptstyle \tilde{\rm O}_{\rm m}} \\ X & \xrightarrow[\quad F \quad]{} & Y \end{array} \ , \tag{11}$$

which is nearly commutative in the sense that

$$\mathrm{tr}\left(\sqrt{\mathrm{E}_{F(x)}}P^{\mathcal{M}}(\mathrm{I}_{\mathrm{m}}(x))\sqrt{\mathrm{E}_{F(x)}}\right) > 1-(p+\alpha)\ , \quad (12)$$

where $\tilde{\mathrm{I}}_{\mathrm{m}} \equiv \mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}}\circ \mathrm{I}_{\mathrm{m}}$, $\tilde{\mathrm{O}}_{\mathrm{m}} \equiv \mathrm{O}_{\mathrm{m}}\circ\mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}}$, *and* $P^{\mathcal{M}} \equiv \mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}}P\mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}}$.

Proof.

$$\begin{aligned}
&\mathrm{tr}\left(\sqrt{\mathrm{E}_{F(x)}}P^{\mathcal{M}}(\mathrm{I}_{\mathbf{m}}(x))\sqrt{\mathrm{E}_{F(x)}}\right)\\
&\quad= \mathrm{tr}\left(\sqrt{\mathrm{E}_{F(x)}}\{P^{\mathcal{M}}(\mathrm{I}_{\mathbf{m}}(x)) - U\,\mathrm{I}_{\mathbf{m}}(x)U^{\dagger}\}\sqrt{\mathrm{E}_{F(x)}}\right)\\
&\quad+\mathrm{tr}\left(\sqrt{\mathrm{E}_{F(x)}}U\,\mathrm{I}_{\mathbf{m}}(x)U^{\dagger}\sqrt{\mathrm{E}_{F(x)}}\right)\\
&\quad> -\alpha+1-p.
\end{aligned}$$

□

Diagram (11) relates the actual implementation P of the quantum computation to the intended classical computation F. The above result implies that a *quantum* computer realization, P, satisfying the QCC and hence operating fault-tolerantly in the presence of residual errors, correctly implements an instance of a *classical* probabilistic computation. In the case Y is binary, the classical probabilistic computation succeeds by majority voting if $\alpha + p < 1/2$. Note that in the idealized limit in which error correction *perfectly* and *permanently* removes all residual errors (*i.e.*, in the limit $\alpha = 0$), our result reduces to the corresponding result of the Kitaev model (*i.e.*, eq.(12) reduces to eq.(9)). This concludes our extension of the Kitaev model.

Elaborating on this result, we see from the stability result of Proposition 1, that implementation of the classical computation is stable under small perturbations in the SO norm of P [12]. The use of the SO norm in the statement of the QCC allows us to make the strongest possible statment of Theorem 1 above. By Theorem 9.1 of [13], for any trace preserving positive superoperators P and P',

$$\begin{aligned}
&\|P-P'\|^{\mathrm{sa}}_{\mathrm{SO}}\\
&\qquad= \sup_{E,\rho}\sum_{y\in Y}\left|\,\mathrm{tr}\,\sqrt{\mathrm{E}_y}P(\rho)\sqrt{\mathrm{E}_y} - \mathrm{tr}\,\sqrt{\mathrm{E}_y}P'(\rho)\sqrt{\mathrm{E}_y}\right|
\end{aligned} \quad (13)$$

as E varies over POVMs and ρ varies over density matrices. Since the initialization operators $\tilde{\mathrm{I}}_{\mathbf{m}}$ in diagram (11) map to arbitrary density matrices, the SO norm is the smallest norm which can be used in Theorem 1. Thus, the use of the SO norm in the definition of the QCC, as opposed to some alternative operator norm, plays a crucial role in establishing Theorem 1, and hence in quantifying how well the quantum computer performs the desired computation. In particular, the use of the SO norm allows the strongest possible statement of the conditions under which a quantum computation is successful.

DISTINGUISHABILITY, COMPOSABILITY AND THE QCC

The QCC precisely specifies the constraints that must be satisfied in order for a candidate quantum computer design to implement a given unitary transformation, up to a prescribed inaccuracy α. The explicit mathematical statement of the QCC makes use of the SO norm to characterize distances between superoperators. Discussions of the distinguishability and composability of superoperators in the context of quantum information-theoretic applications [9, 14, 15], however, sometimes characterize distances between superoperators using the diamond norm. The diamond norm is defined as follows:

Definition 1 *The diamond norm* $\|P\|_{\diamond}$ *of a superoperator* P *is the supremum of the SO norm of* $P\otimes I_n$ *for every* n. *Obviously the diamond norm is at least as large as the SO norm.*

In this Section we show that physical considerations dictate the use of the SO norm, and not the diamond norm, in the proper statement of the QCC. For purposes of analysis, we will designate a variant "QCC," obtained by replacing the SO norm with the diamond norm, by the symbol $\mathrm{QCC}_{\diamond}$, corresponding to the inequality

$$\|P_Q^{\mathcal{M}} - G_Q\|_{\diamond} \le \alpha\ , \quad (14)$$

where G_Q is the desired (ideal) quantum computation, P_Q is the intended physical implementation, and $P_Q^{\mathcal{M}} \equiv \mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}}P_Q\mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}}$.

We consider a quantum computer that is initially uncorrelated with its environment. The state of the system is then $\rho_{QE} = \rho_Q\otimes\rho_E$, where Q and E denote the quantum computer and the environment, respectively. In this case it makes no difference whether we state the QCC as

$$\forall\rho_Q\ ,\ \|\left(P_Q^{\mathcal{M}} - G_Q\right)\rho_Q\|_1 \le \alpha\ , \quad (15)$$

which is equivalent to the proper QCC under the SO norm, or as

$$\forall\rho_Q\forall\rho_E\ ,\ \|[\left(P_Q^{\mathcal{M}} - G_Q\right)\otimes I_E]\rho_Q\otimes\rho_E\|_1 \le \alpha\ , \quad (16)$$

which is equivalent to the $\mathrm{QCC}_{\diamond}$ restricted to uncorrelated states $\rho_Q\otimes\rho_E$. *With this restriction understood*, the proper QCC, and the variant $\mathrm{QCC}_{\diamond}$, furnish equivalent physical statements.

However, it is *not* true that the proper QCC and $\mathrm{QCC}_{\diamond}$ furnish equivalent physical statements in general, since the diamond norm is not restricted to uncorrelated states. If we were to use the $\mathrm{QCC}_{\diamond}$ instead of the proper QCC, we would inevitably reject quantum computer implementations that do, in fact, give correct results. To see why this is so, consider a completely positive map $P_Q^{\mathcal{M}}$ that satisfies the proper QCC:

$$\|P_Q^{\mathcal{M}} - G_Q\|^{\mathrm{sa}}_{\mathrm{SO}} \le \alpha\ . \quad (17)$$

It follows from Theorem 1 above that the implementation P_Q of the quantum computation gives the desired results. P_Q therefore furnishes a viable implementation of a quantum computer. In spite of this, P_Q does *not* necessarily satisfy the QCC$_\diamond$. In general there are correlated states $\rho_{QE} \neq \rho_Q \otimes \rho_E$ such that

$$\|[(P_Q^{\mathcal{M}} - G_Q) \otimes I_E]\rho_{QE}\|_1 > \alpha \ , \tag{18}$$

as pointed out in [14, 15], and so

$$\|P_Q^{\mathcal{M}} - G_Q\|_\diamond > \alpha \ , \tag{19}$$

which violates the QCC$_\diamond$ (*cf* eq.(14)). Thus, the replacement of the SO norm with the diamond norm in the QCC would result in the erroneous rejection of an acceptable implementation.

In other words, the QCC$_\diamond$ is a *sufficient* condition for the successful implementation of a quantum computation, but it is not a *necessary* condition. With the SO norm the proper QCC provides both a sufficient and necessary condition for successful quantum computation [16]. The SO norm is clearly the correct norm to use in stating the QCC.

The diamond norm may nevertheless be useful for certain mathematical applications. For example, when considering the decomposition of a system into constituent components as a purely mathematical problem, one must consider the fact that, for arbitrary superoperators Q_A and Q'_A, $\|[(Q_A - Q'_A) \otimes I_B]\rho_{AB}\|_1$ may be very large even when $\| (Q_A - Q'_A) \, \mathrm{Tr}_B \rho_{AB}\|_1$ is very small [14, 15]. Mathematical distinguishability in this context would call for the use of the diamond norm [9].

Based on the preceding paragraph, it might appear that physical problems involving the analysis of constituent parts of a quantum computer should be expressed in terms of the QCC$_\diamond$. However, it is crucially important to note that, due to the definition of the diamond norm, the QCC$_\diamond$ can provide a rigorously correct description of the dynamics only in the idealized scenario in which the states of the constituents remain *fully* uncorrelated from the environment for the duration of the quantum computation. Since correlations with the environment will typically occur in any practical implementation, the QCC$_\diamond$ cannot characterize the physics in such circumstances. In summary, although the diamond norm provides the correct *mathematical* description for the problem of splitting a component into constituent parts, the QCC$_\diamond$ does not provide the correct *physical* solution to the corresponding problem [17].

CONCLUSION

We have shown on the basis of the stability properties of the QCC that realistic quantum computation is possible despite variations in system parameters. We then used the QCC to extend Kitaev's model to show that reliable classical computation can be carried out using as input the results of fault-tolerant, but imperfect, quantum computation. We showed that the use of the SO norm in the statement of the QCC plays a critical role in establishing this relationship between quantum and classical computation by providing the strongest possible statement of the accuracy result. We also demonstrated that replacement of the SO norm by the diamond norm leads to the erroneous rejection of acceptable implementations. These properties of the SO norm indicate unambiguously that it is the correct choice for measuring distances between superoperators in the context of the QCC. Finally, we contrasted the QCC problem with the problem of composability of quantum operations. Although the diamond norm provides the correct mathematical description for the problem of splitting a component into constituent parts, we note that the QCC$_\diamond$ (based on the diamond norm), does not provide the correct physical solution to the corresponding problem since it is incompatible with correlations with the environment.

ACKNOWLEDGEMENTS

This research was supported under MITRE Technology Program Grant 07MSR205. We would like to thank D Gottesman and D Lidar for helpful comments.

[1] G. Gilbert, *et al.*, *arXiv:quant-ph/0507141*.
[2] The superoperators $\mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}}$ and $\mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}}$ are noiseless operations and do not represent transformations carried out by physical devices. These superoperators are *linking maps* that are mathematically required to relate states in the logical space H_{logical} to states in the computational space H_{comp}. Since physical encoding and decoding operations must be performed by physical devices and are therefore subject to noise, such physical operations are properly a part of the operation described by P and *not* of $\mathcal{M}_{\{\mathrm{l}\to\mathrm{c}\}}$ and $\mathcal{M}_{\{\mathrm{c}\to\mathrm{l}\}}$.
[3] J. Preskill, Proc. Roy. Soc. Lond. A **454**, 385 (1998).
[4] D. A. Lidar, D. Bacon, K. B. Whaley, Phys. Rev. Lett. **84**, 4556 (1999).
[5] G. Gilbert, *et al.*, *arXiv:quant-ph/0510116*.
[6] The quantum computational implementation inaccuracy, α, should not be confused with thresholds for fault-tolerant quantum computation. The relationship between them is discussed in [1].
[7] The formulations, results and proofs presented and obtained here will be generalized to the case of non-Markovian underlying dynamics in a subsequent paper. There we will also consider time-dependent generalizations of the operators A, as well as time-dependent *perturbations* of A, and other variations of the dynamical parameters, such as variation in the strong topology instead of the overly restrictive norm topology.
[8] M. Friesen, *et al.*, Appl. Phys. Lett., **81**, 4619 (2002).

[9] A. Kitaev, Russian Mathematical Surveys, **52**, 1191 (1997).

[10] Note that in [14], Kitaev and co-authors discuss gates that may be subject to noise. However, no specific connection between classical and quantum computation is developed in [14]. Our treatment provides quantitative, specific relations between the ideally defined quantum computation, U, the implementation inaccuracy thereof, α, the instability of the actual open quantum system evolution, P, and the success probability, $p + \alpha$, of the classical computation, F.

[11] It is important to note that the probabilistic inaccuracy of the classical computation, p, and the implementation inaccuracy of the quantum computation, α, are independent quantities.

[12] Since the perturbation $P \to P'$ results in the replacement $\alpha \to \alpha'$, stable computation requires that $\alpha' + p < 1/2$.

[13] M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge (2000).

[14] D. Aharonov, *et al.*, Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computation (STOC), 20, (1997).

[15] B. Rogsen, J. Watrous, *arXiv:cs.CC/0407056*.

[16] The QCC is a necessary condition in the sense that the SO norm is the smallest possible norm for which Theorem 1 holds.

[17] We note that the authors of [14] make use of the diamond norm of a difference of superoperators to bound the accumulation of errors in a quantum circuit. However, since their analysis makes use of the diamond norm, their formulation does not properly account for the general situation in which the constituent states become correlated with the environment.